



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.		
10/531,753	09/20/2005	Peter Nesz	P17299-US1	6062		
27045	7590	03/31/2009	EXAMINER			
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR 1-C-11 PLANO, TX 75024				TAHA, SHAQ		
ART UNIT		PAPER NUMBER				
2446						
MAIL DATE		DELIVERY MODE				
03/31/2009		PAPER				

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/531,753	NESZ ET AL.	
	Examiner	Art Unit	
	SHAQ TAHA	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 23 January 2009.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 13 - 22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 13 - 22 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 04/18/2005 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____. | 6) <input type="checkbox"/> Other: _____ . |

DETAILED ACTION

This is a Final action for application number 10/531,753 after a non-final filed 01/23/2009. The original application was filed on 04/18/2005. Claims 13 – 22 are currently pending and have been considered below. Claims 13 – 22 are amended. Claims 13 and 18 are independent claims.

Applicant's Response

Applicant's arguments with respect to claims 13 - 22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 13 – 16, and 18 - 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. (US 6,427,170), in view of Alkhatib et al. (US 2004/0044778) and further in view Lim et al. (US 5,884,024).

Regarding claim 13, Sitaraman et al. teaches a for preventing illegitimate use of an Internet Protocol (IP) address by a subscriber device in an IP network, the network including a switch node and at least one DHCP server, said subscriber device in communication with the switch node, the method including the steps of:

creating a list of trusted ones of the DHCP servers in said switch node, [The **Dynamic Host Configuration Protocol (DHCP) has been developed to provide an automated assignment of IP addresses and to help solve the shortage of IP addresses as shown in Fig. 2, wherein multiple DHCP servers are shown, Ref # 8, and subscribers are the users shown also in Fig. 2, (Sitaraman et al., Col. 3, lines 30-35)],**

transmitting by the subscriber device a DHCP request message for an IP address, [**When a DHCP client computer attempts an Internet connection, it broadcasts a DHCP request asking for any DHCP on the network to provide it with an IP address and configuration parameters, wherein the subscriber here as the client transmit a DHCP message requesting an IP address, (Sitaraman et al., Col. 3, lines 35-40)],**

receiving a reply message by said switch node which carries an assigned subscriber IP address, [**A DHCP server on the network that is authorized to configure this client will offer an IP address by sending a reply to the client, wherein the IP address is a clients IP address, (Sitaraman et al., Col. 3, lines 40-45)],**

analyzing the reply message by aid switch node to be a DHCP message and having a source address from one of the trusted DHCP servers, **[Upon receiving this offer, the client may decide to accept it or wait for additional offers from other DHCP servers on the network. At the end, the client chooses and accepts one offer, and the chosen DHCP server sends an acknowledgment with the offered IP address, wherein when the reply is received it will be analyzed by the client, (Sitaraman et al., Col. 3,lines 39-45)],**

updating a filter dynamically in the switch node, the filter storing an identification of the subscriber device and the assigned subscriber IP address, **[the adapter 16 filters users' home PoP IDs on its own PoP ID, so that the local cache 6 at a PoP receives events for the users having a home PoP ID of that PoP, wherein the adapter is a filter that stores the identification the subscriber, (Sitaraman et al., Col. 10, lines 27-31)],**

comparing in the filter said source IP address with the stored subscriber IP address, **[These "dynamic" IP addresses are compared with static IP addresses that are practically permanently allocated and recorded, typically, in DNS servers, (Sitaraman et al., Col. 4, lines 10-14)],**

Sitaraman et al. fails to teach discarding said frame when said source IP address differs from the stored subscriber IP address,

Alkhatib et al. teaches transmitting a frame from the subscriber using a source IP address, having the sender break the input data up into frames, transmit the frames and

process the acknowledgment frames sent back by the receiver, (**Alkhatib et al.**,

Paragraph 10, page 1),

Alkhatib et al. further teaches discarding said frame when said source IP address differs from the stored subscriber IP address, wherein checking IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address, (**Alkhatib et al., Paragraph 149, page 9**), in order to devices to be reachable so that a host outside of the private network can initiate communication with the mobile computing device, (**Alkhatib et al., Paragraph 19, page 2**),

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Sitaraman et al. by discarding said frame when said source IP address differs from the stored subscriber IP address, wherein checking IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address, (**Alkhatib et al., Paragraph 149, page 9**), in order to devices to be reachable so that a host outside of the private network can initiate communication with the mobile computing device, (**Alkhatib et al., Paragraph 19, page 2**),

The modified Sitaraman et al. fails to teach that the list of DHCP servers is in said switch node, and in said switch node the reply message is analyzed,

Lim et al. teaches a router 106 as shown in Fig. 1, wherein the combination of cable modems 104 and cable router 106 provides a "secure IP relay agent and further shown in Fig. 2, Ref # 202, (**Lim et al., Col. 5, lines 1 - 10**), in order to ensure the

validity of the source address included in the IP header of IP packets that originate at the client systems, (**Lim et al., Col. 5, lines 50 – 55**),

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Sitaraman by including a switch node that receives DHCP request is received, and in said switch node the reply message is analyzed wherein Lim et al. teaches a router 106 as shown in Fig. 1, wherein the combination of cable modems 104 and cable router 106 provides a "secure IP relay agent and further shown in Fig. 2, Ref # 202, (**Lim et al., Col. 5, lines 1 - 10**), in order to ensure the validity of the source address included in the IP header of IP packets that originate at the client systems, (**Lim et al., Col. 5, lines 50 – 55**).

Regarding claim 14, the method according to claim 13, further comprising the step of storing in the filter a subscriber MAC address, [and a home PoP ID for the user, (**Sitaraman et al., Col. 8, lines 12-20**)], a subscriber physical port number, [**one of the check attributes may be the Port-ID attribute carrying a specific value, (Sitaraman et al., Col. 13, lines 39-42)**], a subscriber virtual LAN identity, [**this ping utility only works effectively in a small system such as a LAN and when all users on the network are running their computers, (Sitaraman et al., Col. 3, lines 57-62)**], and a lease time interval for the assigned subscriber IP address, [**the time at which the IP address was allocated (or the lease grant time), expiry time of the IP address (or the lease time), and a home PoP ID for the user, (Sitaraman et al., Col. 8, lines**

12-20)].

Regarding claim 15, the method according to claim 13, wherein the subscriber IP address is statically assigned and handled by the DHCP servers, [The Dynamic Host Configuration Protocol (DHCP) has been developed to provide an automated assignment of IP addresses and to help solve the shortage of IP addresses, wherein the DHCP here is assigned to handle the IP address of the subscriber, (Sitaraman et al., Col. 3, lines 30-35), wherein the dynamic IP addresses are compared with static IP addresses that are practically permanently allocated and recorded in DNS servers, (Sitaraman et al., Col. 4, lines 10-13)].

Regarding claim 16, the method according to claim 14, the method including deleting the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval is out, [the IP address allocation event includes a user name, an IP address allocated to the user, the time at which the IP address was allocated (or the lease grant time), expiry time of the IP address (or the lease time), and a home PoP ID for the user, wherein the DNS server deletes mappings between domain names and IP addresses from its association database in response to IP address revoke events received from said controller memory publisher, (Sitaraman et al., Col. 8, lines 12-20)].

Regarding claim 18, a switch node in an Internet Protocol (IP) network adapted to prevent illegitimate use of an IP address by a subscriber device, the switch node including: at least one port for communication with a subscriber, an uplink port for communication with DHCP servers in the network, [one of the check attributes may be the Port-ID attribute carrying a specific value, (Sitaraman et al., Col. 13, lines 39-42)],

and a filter device having a list of trusted ones of the DHCP servers, the filter device being associated with the ports, **[The Dynamic Host Configuration Protocol (DHCP) has been developed to provide an automated assignment of IP addresses and to help solve the shortage of IP addresses as shown in Fig. 2, wherein multiple DHCP servers are shown, Ref # 8, (Sitaraman et al., Col. 3, lines 30-35)],**

wherein: the switch node operative to receive a subscriber IP address request message from a subscriber device, analyze it to be a DHCP request message and transmit it on the uplink port, **[A DHCP server on the network that is authorized to configure this client will offer an IP address by sending a reply to the client, wherein the IP address is a clients IP address, (Sitaraman et al., Col. 3, lines 40-45)],**

receive a reply message on the uplink port, analyze it to be a DHCP reply message and having a source IP address from one of the trusted DHCP servers on the list, **[Upon receiving this offer, the client may decide to accept it or wait for additional offers from other DHCP servers on the network. At the end, the client chooses and accepts one offer, and the chosen DHCP server sends an**

acknowledgment with the offered IP address, wherein when the reply is received it will be analyzed by the client, (Sitaraman et al., Col. 3,lines 39-45)],

dynamically update the filter with an identification of the subscriber device and a corresponding assigned subscriber IP address contained in the DHCP reply message, [the adapter 16 filters users' home PoP IDs on its own PoP ID, so that the local cache 6 at a PoP receives events for the users having a home PoP ID of that PoP, wherein the adapter is a filter that stores the identification the subscriber, (Sitaraman et al., Col. 10, lines 27-31)],

compare in the filter said source IP address with the stored subscriber IP address for the subscriber device, [These "dynamic" IP addresses are compared with static IP addresses that are practically permanently allocated and recorded, typically, in DNS servers, (Sitaraman et al., Col. 4, lines 10-14)],

Sitaraman et al. fails to teach discarding said frame when said source IP address differs from the stored subscriber IP address,

Alkhatib et al. teaches transmitting a frame from the subscriber using a source IP address, having the sender break the input data up into frames, transmit the frames and process the acknowledgment frames sent back by the receiver, (Alkhatib et al., Paragraph 10, page 1),

Alkhatib et al. further teaches discarding said frame when said source IP address differs from the stored subscriber IP address, wherein checking IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address, (Alkhatib et al., Paragraph 149, page 9), in order to devices to be

reachable so that a host outside of the private network can initiate communication with the mobile computing device, (**Alkhatib et al., Paragraph 19, page 2**),

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Sitaraman et al. by discarding said frame when said source IP address differs from the stored subscriber IP address, wherein checking IP address in incoming packets, rejecting those in which the source IP address is different than the destination IP address, (**Alkhatib et al., Paragraph 149, page 9**), to devices to be reachable so that a host outside of the private network can initiate communication with the mobile computing device, (**Alkhatib et al., Paragraph 19, page 2**),

The modified Sitaraman et al. fails to teach that the list of DHCP servers is in said switch node, and in said switch node the reply message is analyzed,

Lim et al. teaches a router 106 as shown in Fig. 1, wherein the combination of cable modems 104 and cable router 106 provides a "secure IP relay agent and further shown in Fig. 2, Ref # 202, (**Lim et al., Col. 5, lines 1 - 10**), in order to ensure the validity of the source address included in the IP header of IP packets that originate at the client systems, (**Lim et al., Col. 5, lines 50 – 55**),

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Sitaraman by including a switch node that receives DHCP request is received, and in said switch node the reply message is analyzed wherein Lim et al. teaches a router 106 as shown in Fig. 1, wherein the combination of cable modems 104 and cable router 106 provides a "secure IP relay agent and further shown in Fig. 2, Ref # 202, (**Lim et al., Col. 5, lines 1 - 10**), in order

to ensure the validity of the source address included in the IP header of IP packets that originate at the client systems, (**Lim et al., Col. 5, lines 50 – 55**).

Regarding claim 19, the switch node according to claim 18, wherein the switch node further operative to store in the filter a subscriber MAC address, **[and a home PoP ID for the user, (Sitaraman et al., Col. 8, lines 12-20)]**, a subscriber physical port number, **[one of the check attributes may be the Port-ID attribute carrying a specific value, (Sitaraman et al., Col. 13, lines 39-42)]**, a subscriber virtual LAN identity, **[this ping utility only works effectively in a small system such as a LAN and when all users on the network are running their computers, (Sitaraman et al., Col. 3, lines 57-62)]**, and a lease time interval for the assigned subscriber IP address, **[the time at which the IP address was allocated (or the lease grant time), expiry time of the IP address (or the lease time), and a home PoP ID for the user, (Sitaraman et al., Col. 8, lines 12-20)]**.

Regarding claim 20, the switch node according to claim 18, wherein the subscriber IP address comprises a statically assigned address which is handled by the DHCP servers, **[The Dynamic Host Configuration Protocol (DHCP) has been developed to provide an automated assignment of IP addresses and to help solve the shortage of IP addresses, wherein the DHCP here is assigned to handle the IP address of the subscriber, (Sitaraman et al., Col. 3, lines 30-35)]**.

Regarding claim 21, the switch node according to claim 19, wherein the switch node further operative to delete the subscriber identification and the corresponding assigned subscriber IP address from the filter when the lease time interval expires, [the IP address allocation event includes a user name, an IP address allocated to the user, the time at which the IP address was allocated (or the lease grant time), expiry time of the IP address (or the lease time), and a home PoP ID for the user, wherein the DNS server deletes mappings between domain names and IP addresses from its association database in response to IP address revoke events received from said controller memory publisher, (Sitaraman et al., Col. 8, lines 12-20)].

Claims 17 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. (US 6,427,170), in view of Alkhatib et al. (US 2004/0044778) and further in view of Taylor et al. (US 2002/0065919).

Regarding claims 17 and 22, The modified Sitaraman et al. teaches the method in an IP network according to claim 13, the method further comprising the steps of: counting a number of attempts (n) from the subscriber to use an illegitimate IP address, [When a DHCP client computer attempts an Internet connection, it broadcasts a DHCP request asking for any DHCP server on the network to provide it with an IP address and configuration parameters, wherein the attempt to connect to the internet will be counted, (Sitaraman et al., Col. 3, lines 34-39)],

The modified Sitaraman et al. fails to teach sending a warning signal when the number of attempts exceeds a threshold criteria,

Taylor et al teaches comparing the number (n) of the attempts with a threshold number (N), **[DB servers may include circuitry which checks for a time stamp discrepancy which exceeds a particular threshold, and sends a warning message, wherein the numbers are compared with a specific threshold, Taylor et al., Paragraph 131, Page 8)]**,

Taylor et al further teaches sending a warning signal when the number of attempts exceeds a threshold criteria, **(Taylor et al., Paragraph 131, Page 8)**, in order to increase security, **(Taylor et al., Paragraph 167, Page 10)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Sitaraman by comparing the number (n) of the attempts with a threshold number (N), DB servers may include circuitry which checks for a time stamp discrepancy which exceeds a particular threshold, and sends a warning message, wherein the numbers are compared with a specific threshold, **(Taylor et al., Paragraph 131, Page 8)**, and sending a warning signal when the number of attempts exceeds a threshold criteria, **(Taylor et al., Paragraph 131, Page 8)**, in order to increase security, **(Taylor et al., Paragraph 167, Page 10)**.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Shaq Taha** whose telephone number is 571-270-1921. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Jeff Pwu** can be reached on 571-272-6798.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/S. T./

Examiner, Art Unit 2446

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446